CLAIMS

What is claimed is:

1. A method for roaming in a network environment, the network environment comprising a first bridge device at a first location, a second bridge device at a second location, and a mobile device which roams from the first location to the second location, comprising the steps of:

(a) creating a token by the first bridge device, wherein the token comprises an identity of a context associated with the mobile device;

(b) securely providing the token to the mobile device by the first bridge device;

(c) securely providing the token to the second bridge device by the mobile device;

(d) securely providing the token to the first bridge device by the second bridge device;

(e) determining if the token from the second bridge device is authentic by the first bridge device; and

(f) securely providing the context to the second bridge device by the first bridge device, if the token from the second bridge device is authentic.

2. The method of claim 1, wherein the creating step (a) comprises:

(a1) creating a first message by the first bridge device, wherein the first message comprises a first random number encrypted using a public key of the mobile device; and

(a2) creating a second message by the first bridge device, wherein the second message comprises a digital signature for the first random number and the identity, wherein

the token securely provided to the mobile device by the first bridge device comprises the first message and the second message.

3. The method of claim 2, wherein the digital signature is an encrypted hash of the first random number and the identity.

4. The method of claim 2, further comprising:

(a3) creating a third message by the first bridge device, wherein the third message comprises the first random number and the identity encrypted using a public key of the first bridge device, wherein the token securely provided to the mobile device by the first bridge device comprises the first message, the second message, and the third message.

5. The method of claim 2, further comprising:

(a3) storing the first random number and the identity in a storage medium by the first bridge device.

6. The method of claim 1, wherein the securely providing step (c) comprises:

(c1) obtaining a first random number by the mobile device by decrypting a first message of the token securely provided to the mobile device by the first bridge device using a private key of the mobile device; and

(c2) creating a fourth message by the mobile device, wherein the fourth message comprises the first random number encrypted using a public key of the second bridge device, wherein the token securely provided to the second bridge device by the mobile device

comprises the fourth message and a second message.

7. The method of claim 6, wherein the first message was created by the first bridge device, wherein the first message comprises the first random number encrypted using a public key of the mobile device.

8. The method of claim 6, wherein the second message was created by the first bridge device, wherein the second message comprises a digital signature for the first random number and the identity.

9. The method of claim 6, wherein the token securely provided to the second bridge device by the mobile device further comprises a third message, wherein the third message was created by the first bridge device, wherein the third message comprises the first random number and the identity encrypted using a public key of the first bridge device.

10. The method of claim 1, wherein the securely sending step (d) comprises:

(d1) obtaining a first random number by the second bridge device by decrypting a fourth message of the token securely provided to the second bridge device by the mobile device using a private key of the second bridge device;

(d2) creating a fifth message by the second bridge device, wherein the fifth message comprises a second random number encrypted using the first random number; and

(d3) creating a sixth message by the second bridge device, wherein the sixth message comprises the second random number encrypted using a public key of the first

bridge device, wherein the token securely provided to the first bridge device by the second bridge device comprises the fifth message, the sixth message, and a second message.

11. The method of claim 10, wherein the fourth message was created by the mobile device, wherein the fourth message comprises the first random number encrypted using a public key of the second bridge device.

12. The method of claim 10, wherein the second message was created by the first bridge device, wherein the second message comprises a digital signature for the first random number and the identity.

13. The method of claim 1, wherein the securely providing step (d) comprises:

(d1) securely providing the token to the first bridge device by the second bridge device through at least one intermediary device.

14. The method of claim 1, wherein the determining step (e) comprises:

(e1) obtaining a second random number by the first bridge device by decrypting a sixth message of the token securely provided to the first bridge device by the second bridge device using a private key of the first bridge device;

(e2) obtaining the second random number by the first bridge device by decrypting a fifth message of the token securely provided to the first bridge device by the second bridge device using a first random number;

(e3) determining if the second random number from the sixth message is the same

as the second random number from the fifth message; and

(e4) determining if a digital signature from a second message of the token securely provided to the first bridge device by the second bridge device verifies a source of the token.

15. The method of claim 14, wherein the sixth message was created by the second bridge device, wherein the sixth message comprises the second random number encrypted by the second bridge device using a public key of the first bridge device.

16. The method of claim 14, wherein the fifth message was created by the second bridge device, wherein the fifth message comprises the second random number encrypted using the first random number.

17. The method of claim 14, further comprising:

(e5) obtaining the first random number and the identity by decrypting a third message of the token securely provided to the first bridge device by the second bridge device using the private key of the first bridge device, wherein the third message was created by the first bridge device, wherein the third message comprises the first random number and the identity encrypted using a public key of the first bridge device.

18. The method of claim 14, further comprising:

(e5) obtaining the first random number and the identity by the first bridge device from a storage medium.

19. The method of claim 1, wherein the securely sending step (f) comprises:

(f1) encrypting the context associated with the mobile device by the first bridge device using a second random number obtained from decrypting a sixth message of the token securely provided to the first bridge device by the second bridge device; and

(f2) securely sending the encrypted context to the second bridge device.

20. The method of claim 19, wherein the sixth message was created by the second bridge device, wherein the sixth message comprises the second random number encrypted using a public key of the first bridge device.

21. The method of claim 19, further comprising:

(f3) decrypting the context from the first bridge device by the second bridge device using a private key of the second bridge device; and

(f4) creating a new token by the second bridge device from the decrypted context.

22. The method of claim 1, wherein the securely providing step (f) comprises:

(f1) securely providing the context to the second bridge device by the first bridge device through at least one intermediary device, if the token from the second bridge device is authentic.

23. The method of claim 1, wherein the context comprises at least one of:

information on how to maintain a status of a port to which the mobile device is connected;

an identity of a virtual local area network (LAN) to which the mobile device is connected; and

information on how to return packets from the mobile device to various locations throughout the LAN.

24. The method of claim 1, wherein the identity of the context is a number.

25. A method for roaming in a network environment, the network environment comprising a first bridge device at a first location, a second bridge device at a second location, and a mobile device which roams from the first location to the second location, comprising the steps of:

(a) creating a token by the first bridge device, wherein the token comprises:

a first message comprising a first random number encrypted using a public key of the mobile device, and

a second message comprising a digital signature for the first random number and an identity of a context associated with the mobile device;

(b) providing the token to the mobile device by the first bridge device;

(c) decrypting the first message using a private key of the mobile device by the mobile device to obtain the first random number;

(d) creating a fourth message by the mobile device comprising the first random number encrypted using a public key of the second bridge device;

(e) providing a modified token to the second bridge device by the mobile device, wherein the modified token comprises the fourth message and the second message;

(f) decrypting the fourth message using a private key of the second bridge device by the second bridge device to obtain the first random number;

(g) creating a fifth message by the second bridge device comprising a second random number encrypted using the first random number;

(h) creating a sixth message by the second bridge device comprising the second random number encrypted using a public key of the first bridge device;

(i) providing a twice modified token to the first bridge device by the second bridge device, wherein the twice modified token comprises the fifth message, the sixth message, and the second message;

(j) decrypting the sixth message using a private key of the first bridge device by the first bridge device to obtain the second random number;

(k) decrypting a fifth message using the first random number by the first bridge device to obtain the second random number;

(l) determining by the first bridge device if the second random number from the sixth message is the same as the second random number from the fifth message;

(m) determining by the first bridge device if the digital signature from the second message verifies a source of the twice modified token;

(n) encrypting the context of the identity by the first bridge device using the second random number, if the second random number from the sixth message is the same as the second random number from the fifth message and if the digital signature from the second message verifies the source of the twice modified token; and

(o) providing the encrypted context to the second bridge device by the first bridge device.

26. The method of claim 25, wherein the digital signature is an encrypted hash of the first random number and the identity.

27. The method of claim 25, wherein the token created by the first bridge device further comprises a third message comprising the first random number and the identity encrypted using the public key of the first bridge device.

28. The method of claim 25, wherein the creating step (a) further comprises:

(a1) storing the first random number and the identity in a storage medium by the first bridge device.

29. The method of claim 25, wherein the modified token further comprises a third message created by the first bridge device, wherein the third message comprises the first random number and the identity encrypted using the public key of the first bridge device.

30. The method of claim 25, wherein the providing step (i) comprises:

(i1) providing the twice modified token to the first bridge device by the second bridge device through at least one intermediary device, wherein the twice modified token comprises the fifth message, the sixth message, and the second message.

31. The method of claim 25, wherein the encrypting step (n) comprises:

(n1) decrypting a third message using the private key of the first bridge device by the first bridge device to obtain the first random number and the identity, wherein the third

message was created by the first bridge device by encrypted the third message using the public key of the first bridge device.

32. The method of claim 25, wherein the encrypting step (n) comprises:

(n1) obtaining the first random number and the identity from a storage medium by the first bridge device.

33. The method of claim 25, wherein the providing step (o) comprises:

(o1) providing the encrypted context to the second bridge device by the first bridge device through at least one intermediary device.

34. The method of claims 25, further comprising:

(p) decrypting the encrypted context from the first bridge device by the second bridge device using the private key of the second bridge device; and

(q) creating a new token by the second bridge device.

35. The method of claim 25, wherein the context comprises at least one of:

information on how to maintain a status of a port to which the mobile device is connected;

an identity of a virtual LAN to which the mobile device is connected; and

information on how to return packets from the mobile device to various locations throughout the LAN.

36. The method of claim 25, wherein the identity of the context is a number.